

一种防止以太网被攻击的方法

技术领域

本发明涉及网络安全领域，尤其涉及一种防止以太网被攻击的方法。

发明背景

5 当前，网络病毒的破坏性越来越多样化，出现了许多新的破坏手段。对于网络可靠性的攻击就是这些新的破坏手段的一种。这种攻击不以盗取信息为目的，而是针对网络中的漏洞，对网络设备进行攻击，破坏网络的正常通讯，从而造成网络瘫痪，给用户带来更大的损失。对以太网的攻击是这种攻击的一种常见方式。

10 在以前的网络中，以太网多出现在内网之中，而传统的网络管理认为，内网是非常安全的，因此只对于内网的出口设置了网络安全防范策略，而在内网内部并未设置防范措施。同时，由于内网中客户的不同，导致网络管理部门无法实现对内网中的每个用户的网络使用进行监控，这样，随着计算机病毒不断出现新的破坏手段，以及在网络中越来越多地应用了容易被攻击的中低端网络产品，从而使对以太网的攻击更加容易。另外，随着宽带的兴起和新型业务的普及，以太网越来越多地应用于相对于网络管理部门的外网中，以太网接入的宽带小区就是其中一例，在这种情况下，以太网更易受到攻击。

15

对于采用以太网实现通讯的用户来说，一旦以太网受到攻击，造成20 网络瘫痪，即使没有丢失任何有价值的资料，也会造成与网络瘫痪时间成正比的非常大的损失，而对于利用以太网进行工作业务的公司来说，这种损失往往比丢失资料更为严重。

在以太网中，主机的地址通过媒体访问控制（MAC）地址来标识。在发送数据时，需要在数据报文中携带目的 MAC 地址信息和源 MAC 地址信息。以太网的通讯设备，例如交换机，通过 MAC 地址信息来确定数据报文的转发端口。目前的交换机在转发数据报文时都是基于 MAC 5 学习机制的。如图 1 所示，例如个人计算机（PC）1 的 MAC 地址是 MAC1，PC2 的 MAC 地址是 MAC2。当交换机接收到 PC1 发出的数据报文时，记录该报文携带的 MAC 地址信息和接收到的端口信息，也就是建立 MAC1 和 Port1 的对应关系。与此相似，建立 MAC2 和 Port2 的对应关系。这样交换机可以建立所有的主机的 MAC 地址信息和相应端口信息 10 之间的对应关系，并将其存储在 MAC 表中。在图 1 中，这个 MAC 表有两个表项，其中 MAC1 对应 Port1，MAC2 对应 Port2。当交换机接收到需要发送给 PC1 的数据报文时，首先根据 PC1 的 MAC 地址 MAC1 从 MAC 表中查找到相应的端口 Port1，然后将该数据报文通过该端口发送给 PC1。

15 在上述 MAC 地址的学习过程中，没有任何的认证机制，这样恶意用户可以据此对以太网中的单个用户或者整个以太网发起攻击。这种攻击可以通过 MAC 地址欺骗的方法来进行，也可以通过 MAC 地址轰炸的方法来进行。

图 2 示出了进行 MAC 地址欺骗的攻击过程示意图。如图 2 所示，20 如果 PC2 的用户是一个恶意用户并且希望攻击 PC1，那么 PC2 可以向交换机发送一个源 MAC 地址是 PC1 的 MAC 地址 MAC1 的数据报文，这时交换机会进行学习，从而建立 MAC1 和 Port2 的对应关系，也就是说，交换机中的 MAC 表中的 MAC1 和 Port1 的对应关系将在这次学习之后更改为 MAC1 和 Port2 的对应关系。这样，所有希望发送给 PC1 的数据 25 报文都会发送到 Port2，从而发送给 PC2，导致 PC1 不能正常接收信息。

如果恶意用户对以太网中的多台甚至所有的主机都采用同样的方法，那么整个以太网将濒于瘫痪。

除了上述 MAC 地址欺骗的方式之外，恶意用户也可以采用 MAC 地址轰炸的方法来攻击以太网。例如，恶意用户 PC2 可以不断地发出源 5 MAC 地址变化的数据报文，例如在第一个数据报文中 MAC 地址为 MAC1，而在第二个数据报文中 MAC 地址换为 MAC3，在第三个数据报文中 MAC 地址又换为 MAC8。这样每接收到一个数据报文，交换机就需要更新 MAC 表，从而使交换机的 MAC 表始终处于一个不稳定的状态。如果这些源 MAC 地址信息中包含以太网中某个网络设备的真实 10 地址，那么这个网络设备将不能进行正常的通讯。这种方式通常会被病毒所利用，通过被感染病毒的主机对整个以太网进行 MAC 轰炸，从而破坏整个以太网的正常运行。

为了避免上述情况对以太网的攻击，目前在交换机上普遍实行主机 MAC 地址和端口进行绑定。也就是说，在交换机上指定某个端口和某 15 个 MAC 地址建立固定的对应关系，不再学习任何动态的 MAC 地址，这样 MAC 地址和端口的对应关系不会由于新接收的数据报文而改变，从而使 MAC 表成为一个固定表。这样可以有效地避免 MAC 地址欺骗和 MAC 地址轰炸等攻击现象。

但是，这种 MAC 地址和端口的固定绑定关系具有一个非常大的缺 20 点。具体地说，这种绑定关系需要网络管理员根据固定的网络连接情况对交换机进行设置，而且一旦完成设置以后，这个网络就处于一种固定模式之下。一台新的计算机或者其它的合法以太网设备连接到网络中后不能进行通信，当计算机更换了一块以太网网卡后，由于 MAC 地址的改变，该计算机也不能进行通信，并且，当把计算机从一个地方移动到 25 另一个地方，也可能由于连接端口的改变而无法通信。在这些情况下，

也就是在整个以太网的任何网络设备出现了端口或 MAC 地址变化的情况下，网络管理员必须及时地修改交换机的配置，从而给整个网络维护带来了极大的不便，并且增加了网络维护的成本。

发明内容

5 有鉴于此，本发明的主要目的在于提供一种防止以太网被攻击的方法，该方法可以在保证以太网网络安全的情况下，简化对硬件地址和端口之间的对应关系的配置，增加网络管理的方便性和灵活性，降低网络维护成本。

为了实现上述目的，根据本发明的防止以太网被攻击的方法包括如
10 下步骤：

a. 在以太网通讯设备检测到端口和终端设备的新建连接并接收到来自该终端设备的数据后，建立并保存该端口和该终端设备的硬件地址的固定对应关系，并根据固定对应关系转发数据；

b. 在以太网通讯设备检测到端口和终端设备的连接断开后，删除所
15 保存的固定对应关系。

在上述方法中，在步骤 a 中建立并保存固定关系之前可以进一步包括：在接收到来自该终端设备的数据之后判断是否已经建立了固定关系，如果是，直接转发数据，否则，执行步骤 a 中建立并保存该端口和该终端设备的硬件地址的固定对应关系的步骤。其中，直接转发数据包括：判断数据中携带的硬件地址是否和固定对应关系中该端口对应的硬件地址一致，如果是，按照正常处理流程转发数据；否则丢弃该数据。并且，在丢弃数据之后，可以进一步将判断结果记录在日志中并通知网络管理员。

在上述方法中，硬件地址可以是 MAC 地址。

在上述方法中，检测终端设备和端口的新建连接以及检测终端设备和端口的连接断开是通过检测端口的物理信号进行的。

在上述方法中，通讯设备可以是二层交换机、三层交换机、防火墙设备或以太网桥。终端设备可以是个人计算机、服务器或网际协议（IP）
5 电话机。

在上述方法中，固定对应关系保存在通讯设备的硬件地址表中。

从本发明的技术方案可以看出，在终端设备连接到以太网通讯设备并且发送有数据时，通讯设备学习该端口的硬件地址，从而建立终端设备的硬件地址和该端口的对应关系。而在终端设备断开和通讯设备的连接后，通讯设备会删除该端口所建立的对应关系，在该端口再次连接原始终端设备或者在该端口连接有新的终端设备时，通讯设备再重新通过学习建立硬件地址和端口的对应关系。这样，相对于现有技术中建立固定的对应关系表，对表中表项的修改需要由网络管理员手动完成而言，本发明会自动删除旧的对应关系和建立新的对应关系，从而给网络管理员带来了更大的方便，有效提高了网络维护的效率，降低了网络维护的成本。
10
15

另外，和硬件地址表可以不断更新的情况相比，本发明中一旦建立了硬件地址表，除非检测到终端设备和通讯设备的连接断开，硬件地址表中该端口的对应关系都相对固定，不会接收一次数据就进行一次更改。因此，本发明可以有效地避免现有技术中 MAC 地址欺骗和 MAC 地址轰炸的现象，减小了以太网被攻击的危险，从而提高了网络的安全性和可靠性。
20

附图简要说明

图 1 为 IP 以太网中 MAC 学习机制的示意图。

图 2 为 IP 以太网中 MAC 地址欺骗的攻击过程示意图。

图 3 为本发明的总体处理流程图。

实施本发明的方式

下面结合附图和具体实施例对本发明进行详细说明。

在以太网中，所有的转发数据都是来源于用户层网络中的用户设备，这些用户设备包括 PC、服务器、IP 电话等以太网终端设备，而与这些用户设备相连接的则是接入层的交换机。对于以太网终端设备来说，它们都有各自的 MAC 地址，这个 MAC 地址一般是不会变化的，也就是说，交换机每个端口对应的 MAC 地址一般不会变化。只有在用户更换整个终端设备、更换 PC 中的网卡或者长距离地移动终端设备的情况下，交换机该端口对应的 MAC 地址才有可能变化。而在上述情况下，都需要中断终端设备和交换机的物理连接。在本发明中对交换机采用了 MAC 学习机制，并且通过检测物理信号来检测终端设备和交换机的物理连接是否中断，来决定是否要更新 MAC 表，从而可以使本发明既可以避免例如 MAC 地址欺骗和 MAC 地址轰炸等恶意用户对以太网的攻击，又可以避免固定 MAC 表造成的系统维护不便和维护成本高的缺点。

图 3 示出了本发明的总体处理流程图。下面结合图 3 对本发明进行详细说明。

在一个以太网终端设备和交换机的端口建立连接后，在步骤 301 中，交换机接收来自终端设备的数据报文。

在步骤 302 中，交换机接收到该数据报文后，首先判断接收数据报文的端口是否已经基于 MAC 学习机制在 MAC 表中建立该终端设备的 MAC 地址和相应端口的对应关系，如果还没有针对该终端设备进行 MAC 地址学习，执行步骤 303，否则执行步骤 305。

在步骤 303 中，交换机的端口进行 MAC 地址学习，也就是在 MAC 表中建立该终端设备和该端口之间的对应关系。

在步骤 304 中，按照现有技术转发数据报文的处理过程正常转发该数据报文。

5 在步骤 305 中，判断数据报文中的源 MAC 地址是否和 MAC 表中该端口对应的 MAC 地址一致，如果一致，表明该数据报文是来自 MAC 表中该终端对应的 MAC 地址所对应的终端设备，执行步骤 304；如果不一致，表明该数据报文可能是恶意用户伪造 MAC 地址所发的数据报文，执行步骤 306，也就是丢弃该报文。在判断出 MAC 地址不一致并
10 10 丢弃报文后，可以进一步将这种不一致的情况记录在日志中并通知网络管理员。

通过上述步骤即完成对一次数据报文的转发，然后在步骤 307 中，
15 交换机判断连接该端口的终端设备是否和交换机断开连接。如果连接断开，在步骤 308 中，交换机在当前的 MAC 表中删除和该端口相关联的
MAC 表项，也就是删除当前的终端设备的 MAC 地址和端口的对应关系，
当前处理结束。如果在该端口再次连接有终端设备，例如是另一个终端设备，是同一个终端设备但更换了网卡，或者依然是原来的终端设备并且网卡也没有更换，都重新开始本发明的处理流程，也就是重新建立该端口连接的终端设备的 MAC 地址和该端口之间的对应关系。如果连接
20 没有断开，则重复执行步骤 301 及其后续步骤。

在本发明中，检测终端设备和端口是否建立有连接是通过检测端口的物理信号来进行的。具体地说，当终端设备和端口建立连接并且在终端设备上电启动后，交换机可以通过端口检测到一个高电平，表示终端设备上电启动。而当终端设备和端口断开连接，包括终端设备断电的情况，
25 交换机可以通过端口检测到低电平，从而表示终端设备已经断开了

交换机端口的连接，这时交换机就会删除 MAC 表中原有对应该端口的表项。

在本发明中，通过基于 MAC 学习机制来建立终端设备的 MAC 地址和交换机端口之间的对应关系，避免了 MAC 地址信息和端口固定绑定
5 所带来的维护效率低和成本高的缺点，同时只要终端设备和端口没有断开连接，MAC 地址表中和该端口对应的表项就不会更改，这样在 PC 上运行伪造 MAC 地址的软件将不会影响交换机的 MAC 表，从而避免了 MAC 地址欺骗和 MAC 地址轰炸等现象。因此本发明通过终端设备和端口的动态绑定，既提高了网络的安全性和可靠性，又提高了网络的维护
10 效率，降低了维护成本。

本领域技术人员可以理解，本发明中的交换机可以是二层交换机，也可以是三层交换机，并且本发明并不局限于交换机，而可以是任何通讯设备，例如基于 MAC 学习的防火墙设备、以太网桥设备等。

因此，以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。
15

权利要求书

1、一种防止以太网被攻击的方法，至少包括如下步骤：

a. 在以太网通讯设备检测到端口和终端设备的新建连接并接收到来自该终端设备的数据后，建立并保存该端口和该终端设备的硬件地址的固定对应关系，并根据所述固定对应关系转发数据；

b. 在以太网通讯设备检测到端口和终端设备的连接断开后，删除所保存的所述固定对应关系。

2、根据权利要求 1 所述的方法，其特征是，在步骤 a 中建立并保存所述固定关系之前进一步包括：在接收到来自该终端设备的数据之后判断是否已经建立了所述固定关系，如果是，直接转发数据，否则，执行步骤 a 中建立并保存该端口和该终端设备的硬件地址的固定对应关系的步骤。

3、根据权利要求 2 所述的方法，其特征是，所述直接转发数据包括：判断数据中携带的硬件地址是否和所述固定对应关系中该端口对应的硬件地址一致，如果是，按照正常处理流程转发数据；否则丢弃该数据。

4、根据权利要求 3 所述的方法，其特征是，在丢弃数据之后进一步包括：将判断结果记录在日志中并通知网络管理员。

5、根据权利要求 1 所述的方法，其特征是，所述硬件地址是媒体访问控制（MAC）地址。

20 6、根据权利要求 1 所述的方法，其特征是，所述检测终端设备和端口的新建连接以及检测终端设备和端口的连接断开是通过检测端口的物理信号进行的。

7、根据权利要求 1 所述的方法，其特征是，所述通讯设备是二层交换机、三层交换机、防火墙设备或以太网桥。

8、根据权利要求 1 所述的方法，其特征是，所述终端设备是个人计算机、服务器或网际协议（IP）电话机。

9、根据权利要求 1 所述的方法，其特征是，所述固定对应关系保存在通讯设备的硬件地址表中。

1/2

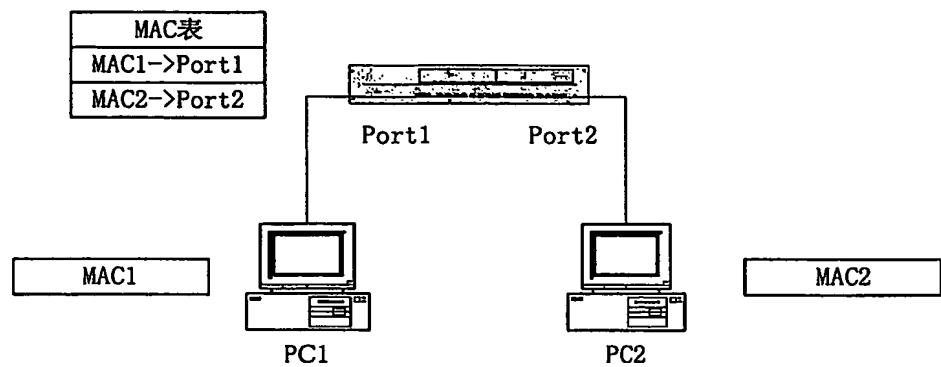


图 1

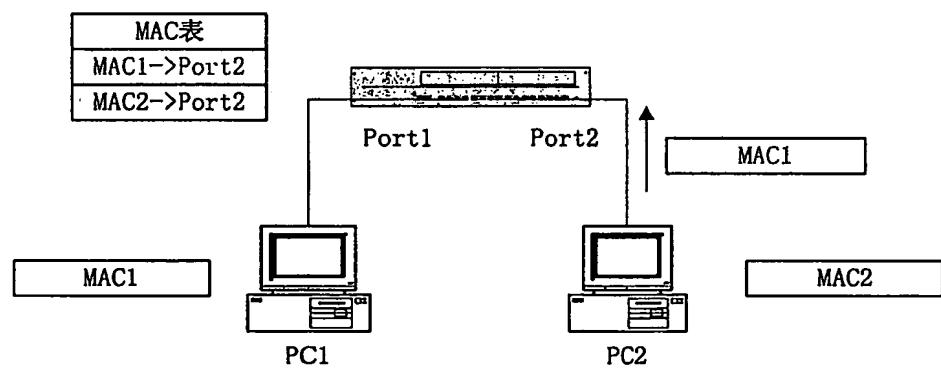


图 2

2/2

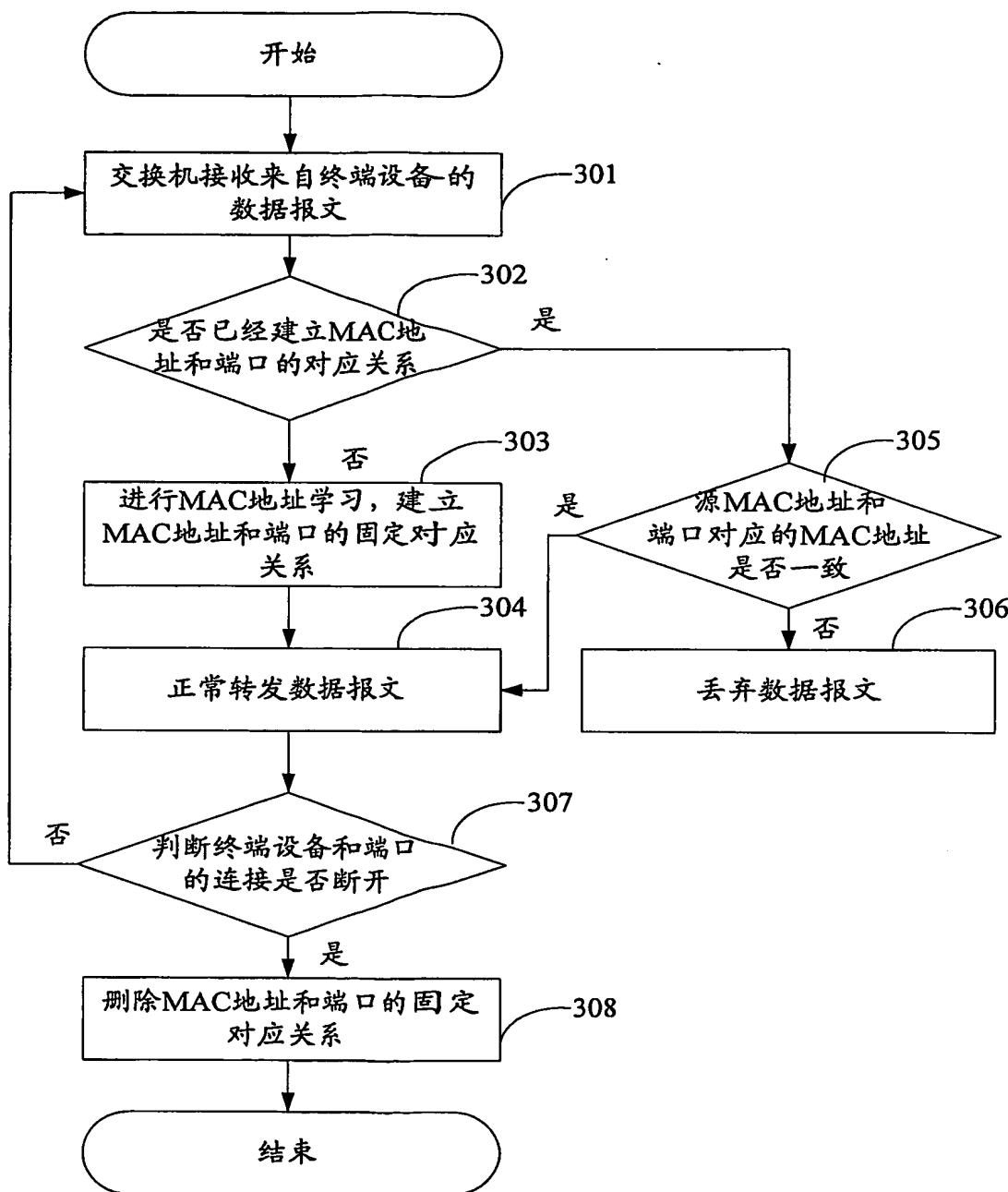


图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2004/000997

A. CLASSIFICATION OF SUBJECT MATTER

IPC⁷: H04L12/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC⁷: H04L12 H04L9

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, PAJ, CNPAT, 中国期刊全文库:

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN1411209A 16.Apri 2003 (HUAWEI TECHNOLOGIES CO.,LTD) see the whole	1—9
A	US20030033531A 13.Feb. 2003 (Brian D. Hanner,Campbell,CA) see the whole	1-9

Further documents are listed in the continuation of Box C. See patent family annex.

<ul style="list-style-type: none"> * Special categories of cited documents: <p>“A” document defining the general state of the art which is not considered to be of particular relevance</p> <p>“E” earlier application or patent but published on or after the international filing date</p> <p>“L” document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>“O” document referring to an oral disclosure, use, exhibition or other means</p> <p>“P” document published prior to the international filing date but later than the priority date claimed</p>	<p>“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>“&” document member of the same patent family</p>
---	---

Date of the actual completion of the international search 23.Nov.2004	Date of mailing of the international search report 30 · DEC 2004 (30 · 12 · 2004)
Name and mailing address of the ISA/ 6 Xitucheng Rd., Jimen Bridge, Haidian District, 100088 Beijing, China Facsimile No. 86-01-62019451	Authorized officer SUN YUFANG Telephone No. 86-01-62084553

INTERNATIONAL SEARCH REPORT

Information patent family members

Search request No.
PCT/CN2004/000997

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
CN1411209A	16.Apri 2003	NONE	
US20030033531A	13.Feb. 2003	NONE	

国际检索报告

国际申请号

PCT/CN2004/000997

A. 主题的分类

IPC⁷: H04L12/24

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC⁷: IPC⁷: H04L12 H04L9

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词 (如使用)

WPI, EPODOC, PAJ, CNPAT, 中国期刊全文库:

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	CN1411209A 16.4 月 2003	(华为技术有限公司) 全文
A	US20030033531A 13.02 月 2003	(Brian D. Hanner,Campbell,CA) 全文

 其余文件在 C 栏的续页中列出。 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“B” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期 23.11 月 2004 (23.11.2004)	国际检索报告邮寄日期 30 12月 2004 (30.12.2004)
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号: (86-10)62019451	受权官员 孙玉芳 电话号码: (86-10)62084553

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2004/000997

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN1411209A	16.4 月 2003	无	
US20030033531A	13.2 月 2003	无	